RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: GRC-W09

AI Governance in Action: Balancing Innovation and Risk in the Age of GenAI

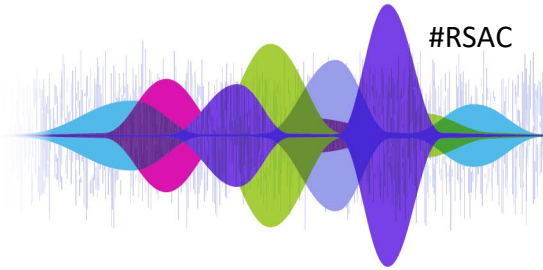
James Christiansen

CISO Advisor, Board member, Mentor, Author,
Netskope

Jim Routh

Board member, Advisor, Mentor, Faculty member
Chief Trust Officer, Saviynt

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

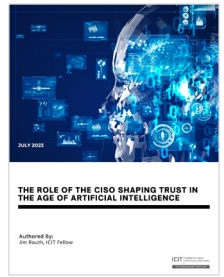
Our Backgrounds

James Christiansen

- Former CSO/CISO
  VISA GM Experian teradata. netskope
- Founder CEO, Evantix, Riskydata
- Advisor Netskope
- Advisory Board Member (3)
- Author & Patent Inventor
- Innovation Award Winner (4)

Jim Routh

- Former CSO/CISO 6x
  AMERICAN EXPRESS DTCC KPMG aetna CVS pharmacy MassMutual
- Former board member
  FS-ISAC & H-ISAC
- Chief Trust Officer
- Board member (3)
  GLOBAL RESILIENCE FEDERATION SAVVY Accountable Digital Identity ADI Association
- Faculty member,
  ICIT Fellow, & mentor



Session Objectives

1

Learn more about the evolving enterprise governance requirements for the use of **Generative AI/LLMs**

2

Understand the considerations for determining **the CISO's role** using a framework and approach for enterprise GenAI governance

3

Recognize several of the aspects of the **"shifting sands"** of the extended attack surface for the use of LLMs in the enterprise

Generative AI: The Big Bang!

Organizations need to develop a **responsible AI framework.**

53% of Americans have used LLMs and 81% use them for personal tasks

92% of Fortune 500 firms have adopted the use of LLMs

21% of consumers use GenAI for creating software code and 85% of those in high tech are using LLMs for automatic code generation.

The most popular use cases include:

- Research & brainstorming (64%)
- First drafts of written content (44%)
- Visuals/graphics for presentations (36%)

SOURCE: GT Edge Platform using Perplexity 2/14/2025

JSC => JR

Helpful Definitions

This type of AI models have been in use for more than a decade

AI

- ANI (AI- Narrow)
- AGI (AI- General)
- ASI (AI- Super)

ML

- Supervised Learning
- Un-Supervised Learning
- Deep Learning
- Reinforcement Learning

Generative AI [GenAI]

Public LLMs are offered to digital consumers

- Text LLM
- Images
- Audio
- Multi-Modal

Inference Infrastructure

Borrowed from Caleb Sima
https://lnkd.in/g5Sf2Wqz

Key components of an AI Governance Program

- Governance Committee
- Use Case Development
- Principles, Policies, Guidance
- Ethical Use, and Regulatory Guidance
- Risk Management
- Data Governance
- Program Oversight and Monitoring

Enablement

- AI – Data Ready
- AI – Security Ready
- AI – Governance Ready

Governance Committee Objectives

- Provide strategic oversight
- Provide a mechanism for checks and balances including human oversight
- Track and articulate business use cases

- Provide governance for all AI/ML initiatives
- Develop the principles, practices and policies
- Provide an ethical compliance framework

- The ability to put containment in place for AI-generated programs
- Promote GenAI education of board and executive committees
- Oversight for accountability, compliance, tracking, and/or monitoring

- Monitor use of GenAI and associated LLMs across platforms and services
- Report on all AI programs, the use of AI, and legal and regulatory challenges
- Report on KPIs as defined by programs

- Define clear roles i.e. Chair, Security, Business Operations, Legal, Privacy, Technology, Marketing, decision makers, SMEs and observers

Sample Principles

Customer data will be excluded from foundation LLMs

Access to foundation LLMs will be controlled

The integrity of foundation LLM output is part of the ML system owner's responsibilities

Don't use LLMs for work that requires a consistent and deterministic outcome

Business process owners are accountable for the resilience of LLM output used to support that business processes

Data scientist that use LLMs are accountable for the resilience of the LLM output for embedded models in applications

RSAC 2025 Conference
JR => JR

Sample Practices

Encourage all employees to explore and learn from LLM usage withing SaaS

Explain that LLMs appear to apply judgment to content but are not able to by design

Publish an accountability model for the enterprise

Explore the use of AI Sec tools for filtering models and recording all transactions

Record the use cases of LLMs and SaaS applications using LLMs

Promote accountability of engineers in building ML systems

RSAC 2025 Conference
JR => JSC

Generative AI Use Case Outcomes

Get ready for these…

The LLM output is accurate

The LLM output is accurate and *biased*

The LLM is mostly accurate and *sometimes wrong*

The LLM data set is too big to filter effectively

The code quality generated from an LLM is inconsistent

The prompts ingested sensitive data that leaked

AI and Regulation

The EU AI Act

Executive Order for Safe, Secure and Trustworthy AI

ISO-42001- AI management system standard

China AI Governance

AI is challenging existing legal and regulatory frameworks in two ways

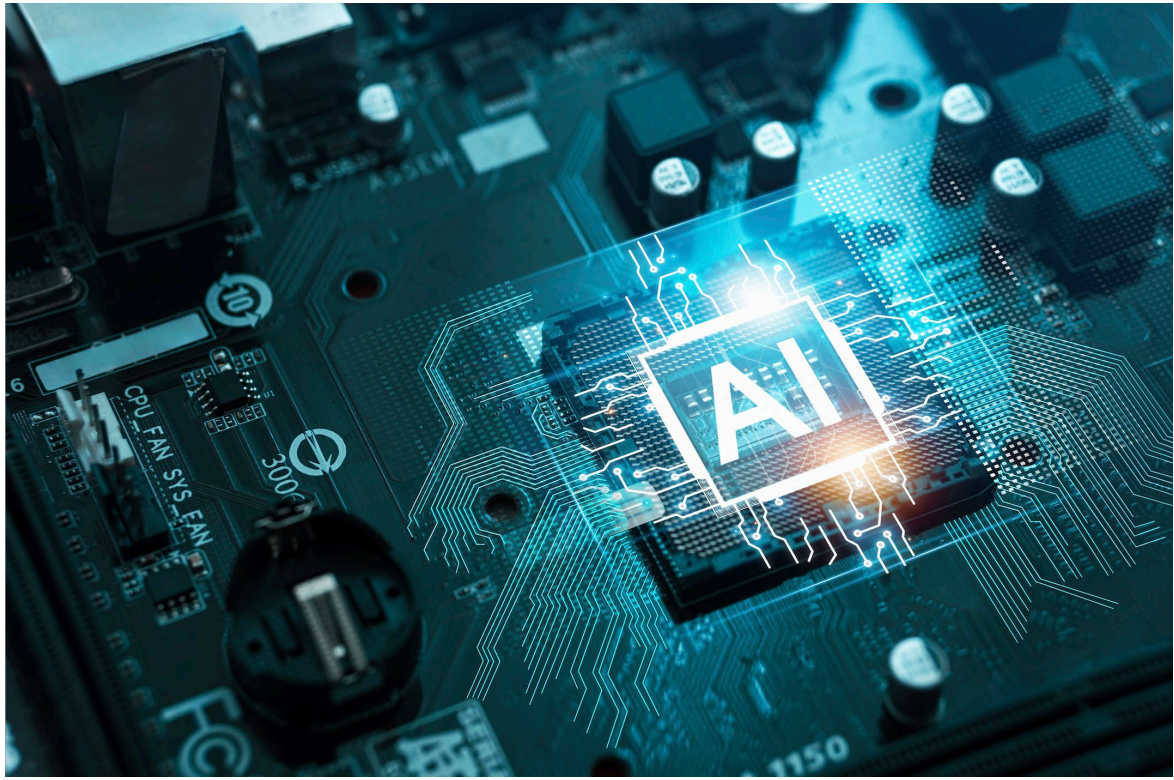
AI's capabilities and shortcomings are inherently different from other technologies
The exponential speed of AI development and the ease of use requires no training

New unregulated threats and risks

Organizations lack the capacity, capability, guidance, and tools needed to safely and confidently deploy AI or manage existing regulatory obligations

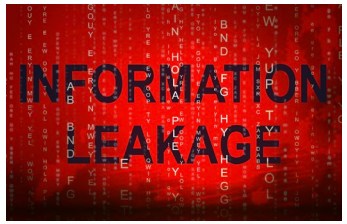
The Role of the CISO in GenAI Governance

- Assist or lead the establishment of a cross-functional team for GenAI governance
- Assist in building business use cases to understand how to use GenAI
- Publish policies/standards and train on use of GenAI based on the principles and practices
- Discover and assess risk of GenAI apps in use
- Update Incident response plans to handle the unique cases for AI, e.g. Hallucinations, etc.
- Use DLP to enforce policies on sensitive data and GenAI usage



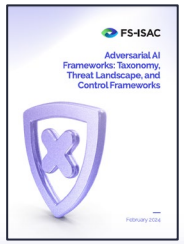
The Evolution of LLM Risk (2 years)

May, 2023



We ***thought*** that data leakage through prompts of public LLMs was the highest risk to the enterprise

May, 2025



We ***know*** that the top risk from LLM usage is data that is wrong

May, 2023

We ***thought*** there would be a surge in use of domain models

May, 2025

ANTHROP\C

Gemini

53% of Americans have used LLMs
81% use them for personal tasks

We ***were*** right on this one

https://berryvilleiml.com/results/

https://www.fsisac.com/knowledge/ai-risk

https://owasp.org/www-project-top-10-for-large-language-model-applications/

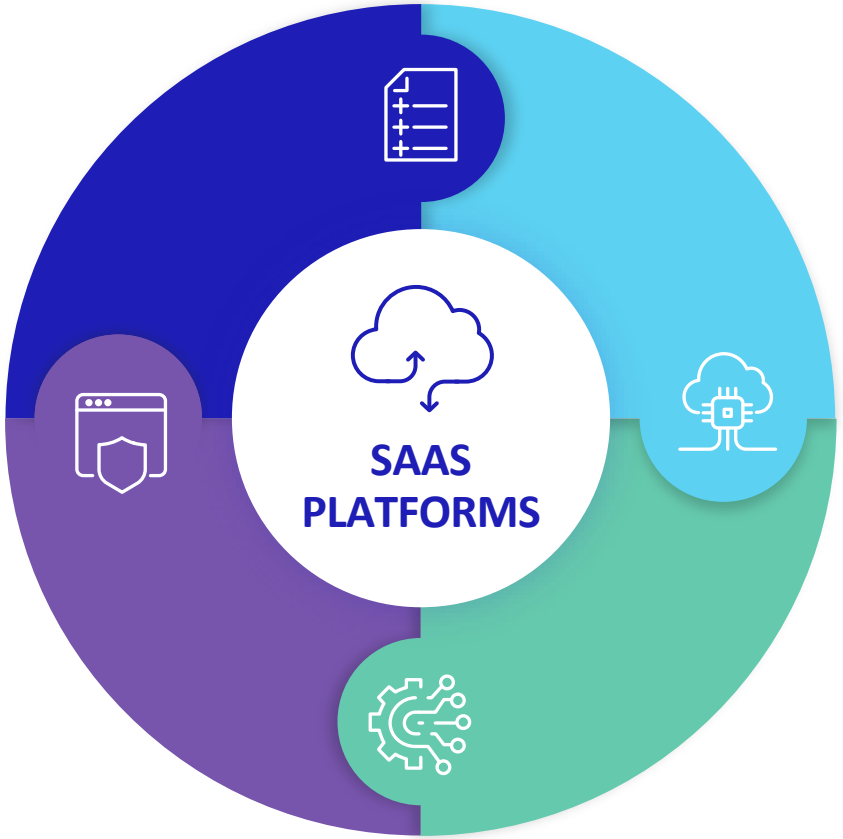
JR => JSC

Third Party Governance

There are thousands of LLMs embedded in SaaS applications and the list is growing

Lack of visibility into third-party AI components creates challenges for governance and accountability

Enforcement of controls should be applied at the Foundational Model level



Enterprises need help identifying the use of LLMs embedded in SaaS applications

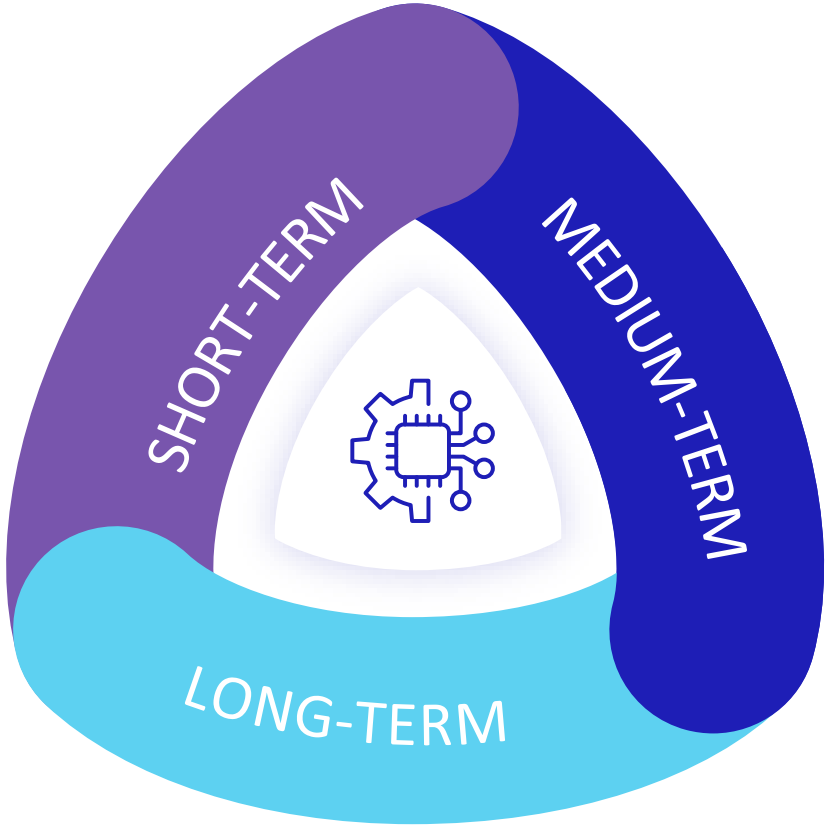
Malicious actors can target AI supply chains to inject vulnerabilities

SaaS vendors must be accountable for the results of the usage of embedded LLMs

- Including LLMs that generate software

Risks Associated with Generative AI

- Accuracy of output (e.g. hallucinations, false information, etc.)
- Data privacy and legal concerns, e.g. copyright
- Bias and Ethical Concerns: Discriminatory hiring decisions, biased financial assessments, etc.
- Model manipulation (OWASP Top 10 AI attacks) and integrity concerns



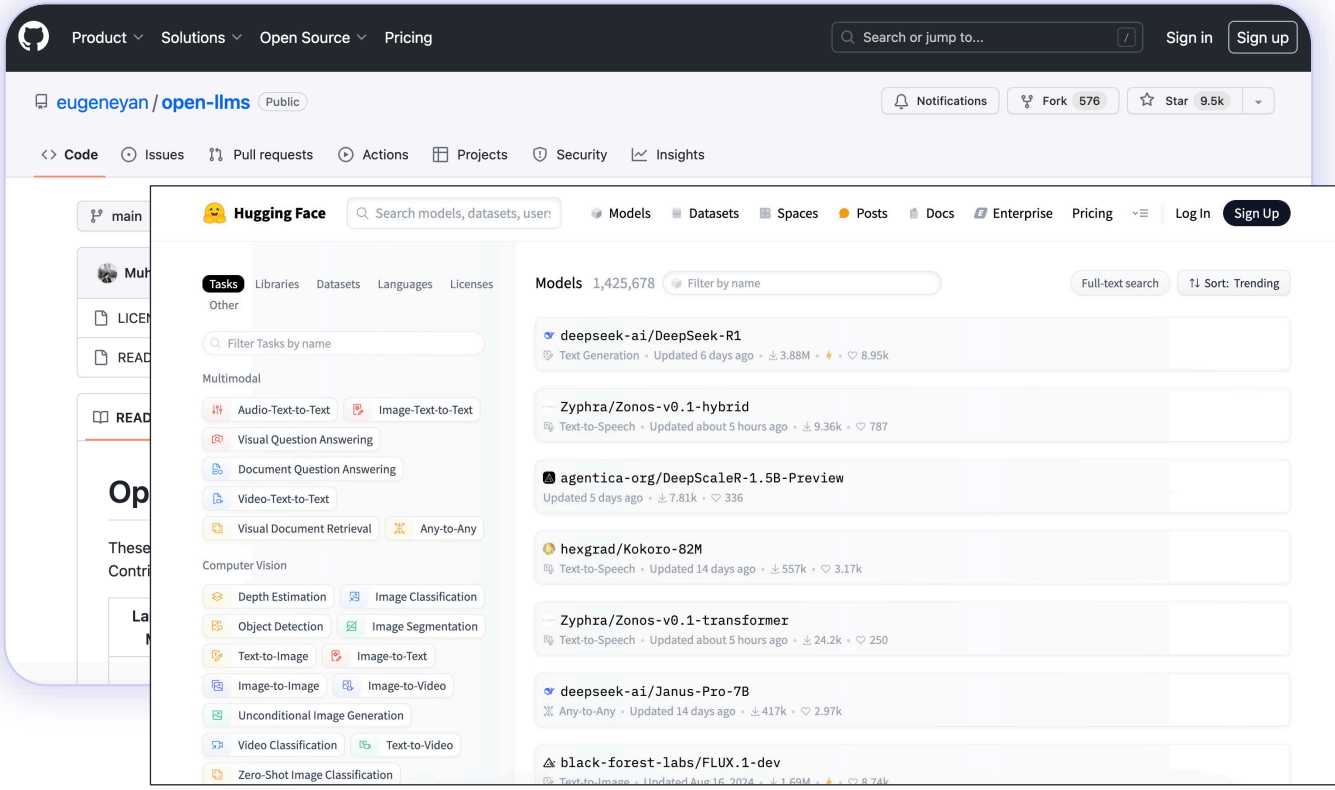
Existential risk to human safety?

- Shifts in workforce skill sets to leverage GenAI appropriately and effectively
- Insecure Third-Party Models: Companies rely on external AI services that may not follow strict security protocols
- Intellectual Property (IP): Who owns AI-generated content?
- Adversarial Attacks & Model Exploits: Prompt Injection, Model Poisoning, Deepfake

https://owasp.org/www-project-top-10-for-large-language-model-applications/

Accountability for LLM Resilience is in the Hands of Developers

- Assembly of software components is like attaching LEGO blocks
- The majority of enterprise usage of LLMs will be through the software build pipeline
- Software engineers must be accountable for the resilience of the software they assemble
- There are lots of choices for developers to deploy GenAI and use it to create code



JR => JR

The Dark Side of LLM usage

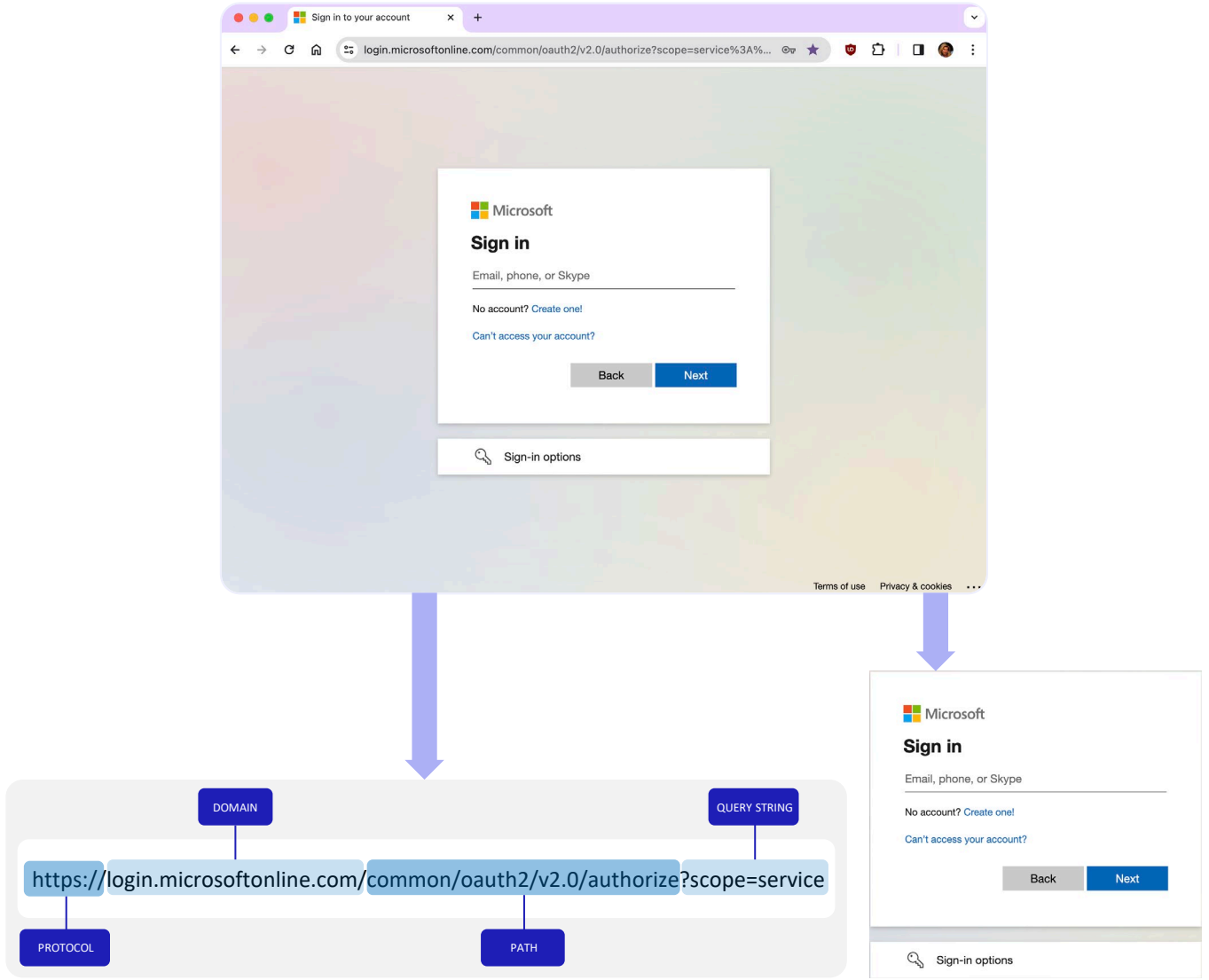
- LLMs make it easier for threat actors to find personal information (emails and social network postings) and **compose compelling phishing** attacks at scale
- LLMs generate software code with malware for things like ransomware attacks
- Deep fake tools are designed to bypass voice and video verification

LLMs to Protect the Enterprise

ML models [including LLMs] are being used to protect enterprises by recognizing behavioral patterns and identifying anomalies [pattern deviation]

A behavior trust score can be generated from models identifying pattern deviation

Orchestrated/automated workflow can be triggered by pattern deviation or trust score



JSC => JR

GenAI KPIs & Reporting

Key Performance Metrics **(KPIs)** measure **the health of the business** process and the underlying control

Sample KPIs

1. #of LLMs in production/total number of applications
2. # of LLMs and ML systems with full observability capability/total ML systems
3. # of use cases documented and reviewed/total use cases discovered

Conclusion

AI is becoming pervasive, and it is changing the way we work

AI is the most rapidly evolving and immersive technology we have ever seen

We are accountable to use AI responsibly

When AI is employed ethically and systematically, there is no cause for alarm

Apply What You Learned

Today

Immediate actions:
Understand the use cases of GenAI and establish interim controls (observability)

90 Days

Establish your GenAI Governance team and program

Focus on three dimensions of attack surface

+90 Days

Monitor the progress of GenAI and establish your metrics for reporting

RSAC 2025 Conference

Thank You!

James Christiansen
James.Christiansen@Netskope.com

Jim Routh
routh3742@gmail.com

JULY 2023
THE ROLE OF THE CISO SHAPING TRUST IN THE AGE OF ARTIFICIAL INTELLIGENCE
Authored By:
Jim Routh, ICIT Fellow
ICIT
Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Many Voices.
One Community.